This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.

+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.

+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.

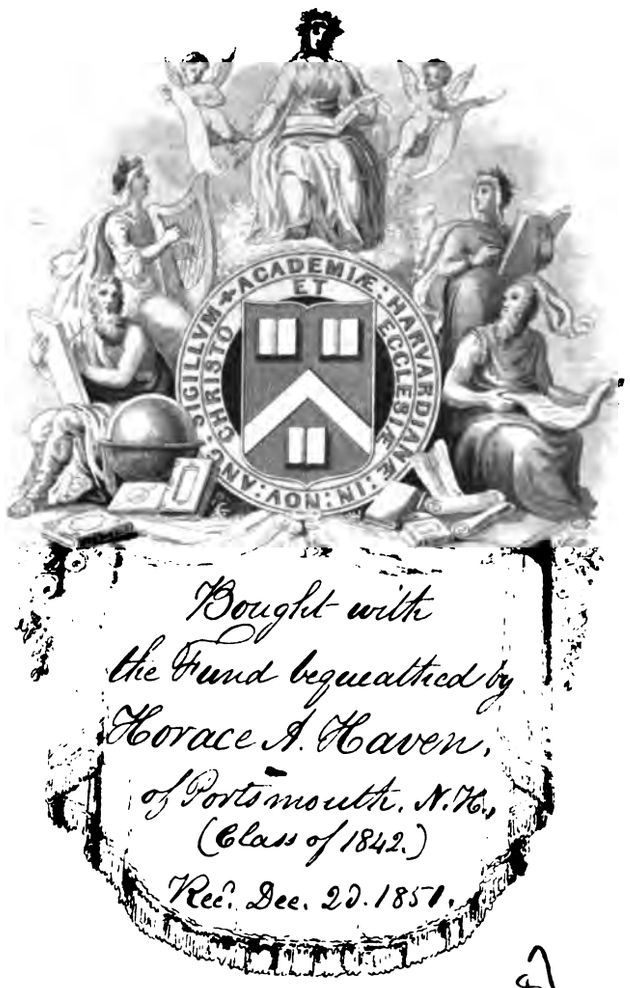
+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

SCIENCE CENTER LIBRARY

Math 1708.44



Bought with
the Fund bequeathed by
Horace A. Haven,
of Portsmouth, N.H.,
(Class of 1842.)
Rec'd. Dec. 22. 1857.

38.87
21

Marginal notes by G. F. Accardi

Breslau, Germany — Universität.

ACADEMIAE

ALBERTINÆ REGIOMONTANÆ

SECULARIA TERTIA

CELEBRANTI

GRATULATUR

ACADEMIA VRATISLAVIENSIS.

Ernst Eduard

ACCEDIT ERNESTI EDUARDI KUMMERI DISPUTATIO DE NUMERIS COMPLEXIS, QUI UNITATIS RADICIBUS ET NUMERIS INTEGRIS REALIBUS CONSTANT.

VRATISLAVIAE

TYPIS UNIVERSITATIS.

MDCCCXLIV.

31.28

Math 1708.44

HARVARD COLLEGE LIBRARY

1851 Dec 2

Bowen Fund

ACADEMIAE VRATISLAVIENSIS RECTOR ET SENATUS

S. P. D.

ACADEMIAE ALBERTINAE REGIOMONTANAE

PRORECTORI MAGNIFICO ET SENATUI ILLUSTRI.

Etsi nullam esse confidimus Germaniae Academiam, quae non magno studio Albertinae vestrae et transacta tria insigni cum laude secula gratuletur et pro pari ejus in posterum incolumitate et gloria vota suscipiat, nos tamen videmur nobis etiam praecipuam quandam causam habere, cur huic officio deesse nolimus. Nam praeter commune illud studiorum fatorumque consortium, quo Germanicae Academiae omnes tamquam firmissimo aliquo amoris vinculo contineri se fatentur, Albertinae vestrae cum nostra Viadrina etiam singularis quaedam necessitudo sortisque similitudo et olim fuit et nunc est. Non enim ignoratis, nostram illam gloriam esse, quod Georgium Sabinum, Philippi Melanchthonis generum, Viadrina nostra habuit professorem et poetam clarissimum, eundemque in publicis negotiis summa cum laude versatum; qui cum apud optimum principem Albertum auctoritate et amicitia plurimum valeret, suo potissimum consilio effecisse videtur, ut Academia vestra conderetur; deinde tamquam colonus a nobis profectus ipsa initia Albertinae diligentissime et sapientissime per decem annos fovit et ornavit, cum quidem per primum triennium rector perpetuus esset, postea iterum tertiumque rector electus, et simul de studiis litterisque optime meritus. Nec silentio praetereundus Christophorus Preiss Pannonius, item Phil. Melanchthonis amicitia clarus, qui apud nos poeticen professus interjecto tempore apud vos eloquentiae et praeceptor et exemplum fuit. Nec defuerunt insequentibus temporibus ac supersunt etiam

hodie viri praestantes, qui utramque Academiam ornaverint. Majus tamen et gravius illud est, quod in terris Borussicis et Brandenburgicis, quae jam tum Sabini maxime opera coalescebant, Academiae vestra ac nostra praecipuae sedes eorum studiorum fuerunt, quibus non solum verior divinarum rerum cognitio confirmata et propagata est, sed reliquae quoque humanae intelligentiae partes, restituta antiqua ingeniorum libertate, quasi ad novam vitam excitatae ingentia ceperunt incrementa. Et vestra quidem Academia cum esset in oris illis constituta, in quibus Sabinus profitebatur ob Scythicae gentis vicinitatem vix civilem vivendi rationem legibus disciplina et imperiis retineri posse, hanc sibi gloriam immortalem peperit, quod promotis quasi eruditi orbis finibus effecit, ut expulsa pristina feritate Borussia vestra eas etiam terras, quae jam antea insigni humanitatis laude floruissent, eadem laude vel aequaret vel superaret. Nobis vero postquam Francofurto Vratislaviam traducti sumus, similis statio obtigit; utrique enim Scythicae, quam Sabinus dicebat, genti vicini in ipsis Germaniae finibus quasdam quasi litterarias excubias agimus et vestro exemplo facimus quod vos et jam dudum fecistis et nunc quoque constantissime agitis, ut, quam e propinquo intuemini hominum vitam tristi torpore oppressam et praetextam potius inani quadam humanitatis specie quam ingenuo liberalis eruditionis amore aequabiliter perfusam, eam quoniam emendare non licet, certe a finibus nostris arceatis. E quo munere hoc vobis commodum redundat, quod

quanto longius estis ob locorum situm ab reliquae Germaniae litterario commercio remoti, tanto id ipsum studiosius amplectimini et defenditis meliusque quanti illud faciendum sit sentitis quam ii qui in media Germania degunt. Quamobrem fit etiam necessario ut acrius doleatis, sicubi animadvertitis existere, qui Palladium illud Germaniae, liberum sanae eruditionis cultum funestis manibus attrectare audeant, sive illi praepostera quadam opinione decepti statuunt aeternum illud humanae intelligentiae veluti flumen subito tardari posse et in ipsorum fallaci sapientia conquiescere, sive privata cupiditate ducti eas ipsas artes dolose impugnant vinculisque injectis etiam evertere conantur, quarum fucatum quendam amorem prae se ferunt. Haec atque talia studia quoniam inter ipsa patriae viscera versantur, plus quam quaevis barbaria extimescenda sunt majoremque desiderant diligentiam et fortitudinem bonorum omnium, inter quos insignem locum vos jam dudum obtinetis. Seculum enim fere est, quod Albertina vestra immortale sibi decus Kantium et adolescentem aluit et deinde virum senemque tenuit, quum ille litteris omnibus optima philosophiae arma praeberet, quibus divinum liberumque animorum motum, in perfectam rerum omnium speciem intentum, ab omni injuria posteri perpetuo defenderent. His vos vestigiis etiam nunc constantissime inceditis eoque facitis, ut dudum partam Albertinae vestrae gloriam non solum conservetis sed etiam augeatis omnesque habeatis vel admiratores vel amicos, qui rempublicam litterariam salvam esse

volunt. Quo animo nos quoque in vos affecti noluimus nostrum desiderari officium in celebranda illius diei solennitate, quo quartum seculum Albertina vestra auspicabitur; quamobrem qui ex animi nostri sententia diem laetissimum vobis gratuletur et optima quaeque apprecetur, legatum misimus Ferdinandum Henricum Abeggium Jurisconsultum, summis apud nos honoribus functum, quem a vobis huc traductum quoniam utrique commune decus habemus, acceptissimum vobis esse certo scimus. Praeterea more a majoribus tradito, ut Academiarum dies festi semper utili aliqua de litteris commentatione celebrentur, Kummeri collegae nostri conjunctissimi mathematicam quandam quaestionem adjunximus, quae nobis in rem propositam eo magis apta visa est, quod testari poterit, quanta pietate quantoque studio Kummerus noster vestrum Jacobium, virum illustrissimum, et veneretur et aemuletur. Valete.

Dab. Vratislaviae Id. Aug. a. MDCCCXLIIII.

DE NUMERIS COMPLEXIS, QUI RADICIBUS UNITATIS ET NUMERIS INTEGRIS REALIBUS CONSTANT.

Numeri complexi, quos summus Gaussius primus in doctrinam numerorum introduxit, et quorum auxilio residuorum biquadraticorum theoriam absolvit, formam habent $a + b\sqrt{-1}$. Praeter hos autem numeros complexos alii etiam innumeri fingi possunt, qui ad alia doctrinae numerorum capita eodem modo pertineant, quo hoc genus simplicissimum numerorum complexorum praecipue ad residua quadratica et biquadratica referendum est. Inter hos praecipue notatu digni videntur numeri complexi altioribus unitatis radicibus, per numeros integros reales multiplicatis, compositi, qui doctrinae de sectione circuli et de residuis potestatum altiorum inserviunt, et cum iis disciplinis tam arcte conjuncti sunt, ut ab ipsis quasi generentur. Quae de iis numeris hactenus in publicum edita sunt summo geometrae Clo. Jacobi debentur, qui primus demonstravit quemlibet numerum primum formae $m\lambda + 1$ in duos factores complexos ejus generis discerpi posse. Quod idem numerus primus p pluribus modis diversis in factores duos diffinditur, et quod producta certa ex iis factoribus formata per alios factores divisibiles fiunt, neque tamen hi ipsi factores cum illis compensari possunt, res maximi momenti, indicat hos factores non esse primos sed compositos. Ulteriorem factorum dissolutionem in factores primos Cl. Jacobi pro iis numeris perfecit, qui radices unitatis quintas, octavas et duodecimas continent, ejusque rei notitiam cum regia academia litterarum Berolinensi communicavit. In hoc quaestionum genere etiam ea versantur, quae Vobis almae universitatis Albertinae viris doctis illustrissimis tanquam magnae meae erga Vos observantiae et reverentiae documentum, hac occasione solemni data, tradere audeo.

§ 1.

Si α est radix quaedam primitiva aequationis $\alpha^\lambda = 1$, quamlibet functionem rationalem integram radicis α, cujus omnes coëfficientes numeri integri sint, numerum integrum complexum voco. Talis functio, aequationis $\alpha^\lambda = 1$ ope, statim ad gradum $\lambda - 1$ reducitur, itaque numerorum complexorum quos tractaturi sumus forma generalis est haec:

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1};$$

numerum λ hic ubique numerum primum accipimus, qui est casus maximi momenti, et quasi fons a quo tota haec doctrina derivatur. Inde rejecta radice $\alpha = 1$, quae hac conditione est sola radix non primitiva, habemus aequationem

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$$

cujus ope ex repraesentatione numeri complexi $f(\alpha)$ unus terminus removeri potest, ex. gr. ultimus, quo facto numerus complexus respectu radicis α ad gradum $\lambda - 2$ deprimitur. Hanc autem reductionem, quae summarum symmetriam turbaret, in universum non adoptabimus, sed retentis omnibus terminis et coëfficientibus a, a_1, a_2, etc. aequatione $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$ ita utemur, ut summa omnium coëfficientium $a + a_1 + a_2 + \ldots + a_{\lambda-1}$ quodam modo in potestate nostra sit. Nam *si coëfficientes numeri complexi $f(\alpha)$ omnes eodem numero augentur vel minuuntur, hic ipse numerus $f(\alpha)$ non mutatur*, quia nihil accedit nisi multiplum formae $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1}$, quae nihilo aequalis est. Vice versa *duo numeri complexi aequales esse nequeunt nisi, coëfficientibus omnibus eodem numero auctis vel minutis, alter prorsus idem fit atque alter.* Positis enim

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$$
$$\varphi(\alpha) = b + b_1\alpha + b_2\alpha^2 + \ldots + b_{\lambda-1}\alpha^{\lambda-1}$$

si est $f(\alpha) = \varphi(\alpha)$ habemus:

$$0 = a - b + (a_1 - b_1)\alpha + (a_2 - b_2)\alpha^2 + \ldots + (a_{\lambda-1} - b_{\lambda-1})\alpha^{\lambda-1}$$

haec autem aequatio gradus $\lambda - 1$ idem valere debet atque aequatio $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$, quia, si res aliter se haberet, ex utraque aequatione conjuncta alia aequatio gradus minoris prodiret, cujus coëfficientes rationales essent, quod fieri non posse ex Gaussii disquisitionibus arithmeticis notum est. Itaque ex aequalitate numerorum $f(\alpha)$ et $\varphi(\alpha)$ sequitur

$$a - b = a_1 - b_1 = a_2 - b_2 = \ldots = a_{\lambda-1} - b_{\lambda-1}.$$

In numero complexo $f(\alpha)$ est α radix quaedam aequationis $1+\alpha+\alpha^2+\ldots+\alpha^{\lambda-1}=0$, cujus ceterae radices unius α potestates sunt, omnibus iis radicibus loco α in $f(\alpha)$ substitutis habemus $\lambda-1$ numeros complexos $f(\alpha)$, $f(\alpha^2)$, $f(\alpha^3)\ldots f(\alpha^{\lambda-1})$, quos *numeros conjunctos* appellabimus. Inter hos bini ad radices reciprocas pertinent, scilicet $f(\alpha^\mu)$ et $f(\alpha^{-\mu})$, quos *numeros reciprocos* vocare convenit. Productum omnium numerorum conjunctorum tanquam functio invariabilis integra omnium radicum aequationis $1+\alpha+\alpha^2+\ldots.+\alpha^{\lambda-1}=0$, semper est numerus realis integer, qui numeri complexi *norma* appellatur. Ex ipsa normae definitione statim perspici possunt propositiones simplices: *numeros conjunctos eandem normam habere*, et *normam producti aequalem esse producto ex normis singulorum factorum*. Numeri complexi $f(\alpha)$ normam, praeeunte Clo. Lejeune-Dirichlet, praeposita littera N designamus, ita ut sit:

$$Nf(\alpha)=f(\alpha)\,f(\alpha^2)\,f(\alpha^3)\ldots.f(\alpha^{\lambda-1})$$

unde hae propositones tali modo exhiberi possunt:

$$Nf(\alpha^r)=Nf(\alpha) \text{ et } N(f(\alpha)\varphi(\alpha))=Nf(\alpha)\cdot N\varphi(\alpha).$$

§ 2.

Si omnes coëfficientes numeri complexi $f(\alpha)$ pro indeterminatis habentur, et productum factorum omnium qui normam constituunt evolvitur, forma homogenea gradus $\lambda-1$ et λ indeterminatorum prodit, quorum vero unus ex arbitrio eligi potest, ita ut $\lambda-1$ numeri indeterminati remaneant. Omnes igitur disquisitiones de numeris complexis pro disquisitionibus de talibus formis gradus $\lambda-1$ totidemque indeterminatorum haberi possunt. De formatione hujus formae notare convenit eam pro aequatione haberi posse, quae ex aequationibus duabus,

$$0=a+a_1\alpha+a_2\alpha^2+\ldots.+a_{\lambda-1}\alpha^{\lambda-1}$$
$$0=1+\alpha+\alpha^2+\ldots.+\alpha^{\lambda-1}$$

quantitate α eliminata, efficitur, quam eandem esse atque aequationem $f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})=0$, ex notissimis regulis algebraicis constat. Alio modo norma tanquam denominator communis invenitur, quem systematis aequationum linearium incognitae evolutae habent. Quales denominatores Cl. Jacobi determinantium nomine ornavit et pluribus locis ingeniosissime tractavit. Accipimus systema aequationum linearium hocce:

$$(A)\qquad \begin{array}{l} ab + a_{\lambda-1}b_1 + a_{\lambda-2}b_2 + \ldots + a_1 b_{\lambda-1} = c + m \\ a_1 b + ab_1 + a_{\lambda-1}b_2 + \ldots + a_2 b_{\lambda-1} = c_1 + m \\ a_2 b + a_1 b_1 + ab_2 + \ldots + a_3 b_{\lambda-1} = c_2 + m \\ \qquad\qquad \vdots \qquad\qquad\qquad\qquad\qquad \vdots \\ a_{\lambda-1} b + a_{\lambda-2} b_1 + a_{\lambda-3} b_2 + \ldots + a\, b_{\lambda-1} = c_{\lambda-1} + m \end{array}$$

cujus incognitae sint $b, b_1, b_2, \ldots . b_{\lambda-1}$, easque aequationes secundum ordinem multiplicamus per $1, \alpha, \alpha^2, \ldots . \alpha^{\lambda-1}$, quo facto summa omnium facile in hanc formam redigitur:

$$(a + a_1\alpha + a_2\alpha^2 + \ldots . + a_{\lambda-1}\alpha^{\lambda-1})(b + b_1\alpha + b_2\alpha^2 + \ldots . + b_{\lambda-1}\alpha^{\lambda-1}) = c + c_1\alpha + c_2\alpha^2 + \ldots . + c_{\lambda-1}\alpha^{\lambda-1},$$

inde positis

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots . + a_{\lambda-1}\alpha^{\lambda-1}$$
$$\varphi(\alpha) = b + b_1\alpha + b_2\alpha^2 + \ldots . + b_{\lambda-1}\alpha^{\lambda-1}$$
$$\psi(\alpha) = c + c_1\alpha + c_2\alpha^2 + \ldots . + c_{\lambda-1}\alpha^{\lambda-1}$$

est

$$f(\alpha) \cdot \varphi(\alpha) = \psi(\alpha)$$

et utraque parte per $f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})$ multiplicata, fit

$$\varphi(\alpha) \cdot Nf(\alpha) = \psi(\alpha) f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})$$

sive

$$\varphi(\alpha) = \frac{\psi(\alpha) f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})}{Nf(\alpha)}$$

ex quo apparet quantitatum $b, b_1, b_2, \ldots . b_{\lambda-1}$, quae formulam $\varphi(\alpha)$ constituunt, denominatorem generalem esse normam $Nf(\alpha)$, uti contendimus.

Quum norma sit forma aliqua gradus $\lambda - 1$ et $\lambda - 1$ indeterminatorum, statim quaestio oboritur de numeris qui hac forma repraesentari possint et qui non possint. Hanc autem quaestionem gravissimam, quae sine dubio inter mysteria doctrinae numerorum maxime recondita referenda est, hactenus non potuimus absolvere, sola haec propositio elementaris ad hanc quaestionem spectans: *normam semper habere formam* $m\lambda + 1$, *vel* $m\lambda$, jam hoc loco, quasi in limine disquisitionum nostrarum, facile demonstrari potest. Quem ad finem adhibemus tres numeros complexos $f(\alpha)$, $\varphi(\alpha)$ et $\psi(\alpha)$, eosdem quibus modo usi sumus, quorum vero

coëfficientes omnes integri sint. Si est $f(\alpha) . \varphi(\alpha) = \psi(\alpha)$ inter coëfficientes horum numerorum complexorum aequationes lineares (A) locum habere debent, iisque additis fit:

$$(a + a_1 + a_2 + \ldots + a_{\lambda-1})(b + b_1 + b_2 + \ldots + b_{\lambda-1}) = c + c_1 + c_2 + \ldots + c_{\lambda-1} + \lambda m$$

quae aequatio in congruentiam pro modulo λ mutata docet: ***summam coëfficientium producti duorum numerorum complexorum producto e summis coëfficientium utriusque factoris congruam esse***, *modulo* λ. Quae propositio facillime ad productum quotcunque factorum extenditur. Norma semper est productum $\lambda - 1$ factorum complexorum, qui easdem coëfficientium summas habent, pro ea igitur productum e summis coëfficientium omnium factorum conflatum in potestatem exponentis $\lambda - 1$ abit, unde habemus:

$$(a + a_1 + a_2 + \ldots + a_{\lambda-1})^{\lambda-1} \equiv Nf(\alpha), \text{ mod. } \lambda.$$

itaque per theorema Fermatianum

$$Nf(\alpha) \equiv 1, \text{ mod. } \lambda,$$

nisi forte sit $a + a_1 + a_2 + \ldots + a_{\lambda-1} \equiv 0$, mod. λ, qua conditone fit $Nf(\alpha) \equiv 0$ mod. λ.

§ 3.

Normae usus insignis est in divisione numerorum complexorum, quippe cujus auxilio divisor complexus semper in divisorem realem mutari potest. Posito enim

$$F(\alpha) = f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})$$

fit

$$\frac{\varphi(\alpha)}{f(\alpha)} = \frac{\varphi(\alpha) F(\alpha)}{Nf(\alpha)}.$$

Si $\varphi(\alpha)$ per $f(\alpha)$ divisibilis est, i. e. si hic quotiens numero integro complexo aequalis est, $\varphi(\alpha) . F(\alpha)$ per numerum integrum realem $Nf(\alpha)$ dividi possit necesse est, numerus autem complexus per numerum realem divisibilis non est, nisi coëfficientes ejus singuli, per hunc numerum divisi, eadem residua habeant. Inde nacti sumus hoc criterium generale, quo dijudicari possit, utrum numerus complexus per alium numerum complexum divisibilis sit, an non: ***Numerus complexus*** $\varphi(\alpha)$ ***per alium numerum*** $f(\alpha)$ ***divisibilis est, si in producto evoluto*** $\varphi(\alpha) f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})$ ***omnes coëfficientes pro modulo*** $Nf(\alpha)$ ***congrui sunt, sin vero hi coëfficientes non omnes congrui sunt,*** $\varphi(\alpha)$ ***certo non divisibilis est per*** $f(\alpha)$.

Alio etiam modo numerorum complexorum divisio perfici potest, ita quidem, ut ad divisionem functionum rationalium integrarum revocetur. Altioribus enim potestatibus radicis α admissis, numerus $\varphi(\alpha)$ infinitis modis diversis repraesentari potest, qui omnes hac forma generali continentur:

$$\varphi(\alpha) - (1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1})\,\psi(\alpha)$$

in qua $\psi(\alpha)$ functionem integram quamcunque designat, quae pro fine singulorum problematum apte eligi poterit. Jam dico *si $\varphi(\alpha)$ per $f(\alpha)$ divisibilis sit, huic numero $\varphi(\alpha)$ semper formam ejusmodi dari posse, ut pro quolibet valore quantitatis α, quae tanquam variabilis spectanda est, divisio succedat et residuum relinquatur nullum.* Per hypothesin quotiens $\frac{\varphi(\alpha)}{f(\alpha)}$ aequalis est numero alicui complexo $F(\alpha)$, itaque

$$\frac{\varphi(\alpha)}{f(\alpha)} = F(\alpha) \text{ sive } \varphi(\alpha) = f(\alpha)\,F(\alpha).$$

Jam signo α in x mutato, videmus functionem rationalem integram variabilis x, $\varphi(x) - f(x)\,F(x)$ evanescere, si x cuilibet radici aequationis $1 + x + x^2 + \ldots + x^{\lambda-1} = 0$ aequalis fit, haec igitur functio integra factorem $1 + x + x^2 + \ldots + x^{\lambda-1}$ habeat necesse est, quare in hanc formam redigi potest

$$\varphi(x) - f(x)\,F(x) = (1 + x + x^2 + \ldots + x^{\lambda-1})\,\psi(x)$$

ex qua theorema enuntiatum sponte manat.

§ 4.

Inter numeros complexos praecipue notatu digni sunt ii, quorum norma est unitas, quos omnes unitatum complexarum nomine designamus. Hae unitates in doctrina numerorum complexorum easdem fere partes suscipiunt, quas aequationis Pellianae $x^2 - Dy^2 = \pm 1$ solutiones in doctrina formarum secundi gradus determinantis positivi agunt. Numerus harum unitatum, excepto solo casu $\lambda = 3$, semper infinitus est, et simili modo ut in solvenda aequatione Pelliana semper unitates quaedam fundamentales dantur, ex quibus ad potestates evectis et inter se multiplicatis infinitus numerus aliarum unitatum deducitur. Simplicissimae unitates sunt ± 1, $\pm\alpha$, $\pm\alpha^2$, $\ldots$ $\pm\alpha^{\lambda-1}$, quae sponte se offerunt, praeter has autem aliae facile inveniuntur, ratione habita numeri complexi $1 + \alpha + \alpha^2 + \ldots + \alpha^{r-1}$, in

quo r est numerus quilibet integer minor quam λ, hic numerus fractionis forma exhibetur hoc modo

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{r-1} = \frac{1-\alpha^r}{1-\alpha}$$

ejusque norma est

$$\frac{(1-\alpha^r)(1-\alpha^{2r})(1-\alpha^{3r})\ldots(1-\alpha^{(\lambda-1)r})}{(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots(1-\alpha^{\lambda-1})}$$

in qua, loco exponentium $r, 2r, 3r, \ldots (\lambda-1)r$ residuis minimis modulo λ substitutis, singuli factores numeratoris iidem fiunt atque denominatoris, quae igitur unitati aequalis est. Quum jam $1+\alpha+\alpha^2+\ldots+\alpha^{r-1}$ sit unitas, et norma producti aequalis producto e normis factorum composito, sequitur ut forma generalis

$$\pm\alpha^k(1+\alpha+\alpha^2+\ldots+\alpha^{r-1})^l(1+\alpha+\alpha^2+\ldots+\alpha^{s-1})^m(1+\alpha+\alpha^2 + \ldots + \alpha^{t-1})^n \ldots$$

pro omnibus numeris $k, l, m, n, \ldots r, s, t$, unitates complexas contineat. Numerus factorum diversorum, qui ad potestates evehendi et multiplicandi sunt, ut diversae unitates obtineantur, itemque numeri r, s, t pro singulis numeris λ accurate definiri possunt, quam vero disquisitionem hoc loco praetereuntes, unitatum proprietatem generalem demonstrabimus, qua in posterum utemur scilicet: *unitates complexas non tam singularum radicum* $1, \alpha, \alpha^2, \ldots \alpha^{\lambda-1}$, *quam periodorum ex binis earum,* $\alpha+\alpha^{\lambda-1}$, $\alpha^2+\alpha^{\lambda-2}$ *etc., functiones lineares esse, si ad factorem accedentem* $\pm\alpha^k$ *non respiciatur,* sive *omnes unitates hanc formam habere*:

$$\pm\alpha^k\left\{c + c_1(\alpha+\alpha^{\lambda-1}) + c_2(\alpha^2+\alpha^{\lambda-2}) + \ldots + c_{\frac{\lambda-1}{2}}\left(\alpha^{\frac{\lambda-1}{2}} + \alpha^{\frac{\lambda+1}{2}}\right)\right\}.$$

E producto $1 = \varphi(\alpha)\varphi(\alpha^2)\varphi(\alpha^3)\ldots\varphi(\alpha^{\lambda-1})$ factorum semissem ex arbitrio eligo, ita tamen ut reciproci in eadem semissi non insint, sed cujuslibet factoris reciprocus in altera semissi reperiatur. Horum factorum productum sit $\psi(\alpha)$, unde alterius semissis productum est $\psi(\alpha^{-1})$, et $\psi(\alpha)\psi(\alpha^{-1}) = 1$. Ponatur

$$\psi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$$

unde

$$\psi(\alpha^{-1}) = a + a_1\alpha^{\lambda-1} + a_2\alpha^{\lambda-2} + \ldots + a_{\lambda-1}\alpha$$

atque ex multiplicatione oriatur

$$\psi(\alpha)\psi(\alpha^{-1}) = A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1}$$

erit $A = a^2 + a_1^2 + a_2^2 + \ldots + a_{\lambda-1}^2$

$A_1 = a a_1 + a_1 a_2 + a_2 a_3 + \ldots + a_{\lambda-1} a$

$A_2 = a a_2 + a_1 a_3 + a_2 a_4 + \ldots + a_{\lambda-1} a_1$

etc. etc.

et summa coëfficientium fit

$$A + A_1 + A_2 + \ldots + A_{\lambda-1} = (a + a_1 + a_2 + \ldots + a_{\lambda-1})^2$$

praeterea quum sit $A + A_1\alpha + A_2\alpha^2 + \ldots A_{\lambda-1}\alpha^{\lambda-1} = 1$, erit $A_1 = A_2 = A_3 = \ldots = A_{\lambda-1} = m$ et $A = m + 1$, itaque $m\lambda + 1 = (a + a_1 + a_2 + \ldots + a_{\lambda-1})^2$

$$\text{et } \pm 1 \equiv a + a_1 + a_2 + \ldots + a_{\lambda-1} \text{ mod. } \lambda$$

horum coëfficientium summa, quae congrua est ± 1 modulo λ, etiam aequalis ± 1 accipi potest, quo facto fit $m = 0$, $A = 1$, et quum A sit summa quadratorum positivorum integrorum $A = a^2 + a_1^2 + a_2^2 + \ldots + a_{\lambda-1}^2$ unitati aequalis fieri non potest nisi unus numerorum a, a_1, a_2 etc., unitati aequalis, ceteri nihilo aequales fiunt, habemus igitur

$$\psi(\alpha) = \pm\alpha^k.$$

Quum $\psi(\alpha)$ alteram factorum semissem normae 1 contineat, hac sola conditione eligendam, ut factores reciproci non insint, semper plura producta $\psi(\alpha)$ erunt, quae unitati simplici $\pm\alpha^k$ aequalia sint. Quorum productorum duo eligo, $\psi(\alpha)$ et $\psi_1(\alpha)$, quae excepto uno factore ceteros omnes eosdem habeant, atque hic solus factor, quo $\psi(\alpha)$ differt a $\psi_1(\alpha)$, sit $\varphi(\alpha^\mu)$, unde factor quem $\psi_1(\alpha)$ continet, neque tamen $\psi(\alpha)$, erit $\varphi(\alpha^{-\mu})$. Inde ex conjunctis aequationibus $\psi(\alpha) = \pm\alpha^k$ et $\psi_1(\alpha) = \pm\alpha^h$ fit $\psi_1(\alpha) = \pm\alpha^{h-k}\psi(\alpha)$, et factoribus communibus sublatis et posito $h - k = m$, est

$$\varphi(\alpha^{-\mu}) = \pm\alpha^m \varphi(\alpha^\mu)$$

quaelibet igitur unitas complexa hoc proprium habet, ut a reciproca sua non differat nisi adjecto factore qui ipse est unitas simplex. Facillime inde theorematis supra propositi veritas perspicitur.

Pro $\lambda = 3$ unitates omnes habere debent formam hanc:

$\varphi(\alpha) = \pm\alpha^k(c + c_1(\alpha + \alpha^2))$ et quia $\alpha + \alpha^2 = -1$, $\varphi(\alpha) = \pm\alpha^k(c - c_1)$

ex quo sequitur ut sit $c - c_1 = 1$, pro hoc igitur casu praeter unitates simplices ± 1, $\pm\alpha$, $\pm\alpha^2$, aliae non dantur.

Pro $\lambda = 5$ unitatum forma generalis haec est:

$$\varphi(\alpha) = \pm\alpha^k(c + c_1(\alpha + \alpha^4) + c_2(\alpha^2 + \alpha^3))$$

quae adhibita aequatione $1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$, et posito $c - c_2 = t$, $c_1 - c_2 = u$ in hanc simpliciorem mutatur:

$$\varphi(\alpha) = \pm\alpha^k(t + u(\alpha + \alpha^4))$$

ex qua fit

$$\varphi(\alpha)\,\varphi(\alpha^2) = \pm\alpha^{3k}(t^2 - tu - u^2)$$

itaque $t^2 - tu - u^2 = \pm 1$. Cognitae hujus aequationis solutiones omnes continentur formis

$$t = \frac{\left(\frac{-1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{-1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}}, \quad u = \frac{\left(\frac{-1+\sqrt{5}}{2}\right)^{n} - \left(\frac{-1-\sqrt{5}}{2}\right)^{n}}{\sqrt{5}}$$

quae, quia $\alpha + \alpha^4 = \frac{-1+\sqrt{5}}{2}$, $\alpha^2 + \alpha^3 = \frac{-1-\sqrt{5}}{2}$ etiam hoc modo repraesentari possunt:

$$t = \frac{(\alpha + \alpha^4)^{n-1} - (\alpha^2 + \alpha^3)^{n-1}}{\alpha + \alpha^4 - \alpha^2 - \alpha^3}, \quad u = \frac{(\alpha + \alpha^4)^{n} - (\alpha^2 + \alpha^3)^{n}}{\alpha + \alpha^4 - \alpha^2 - \alpha^3}$$

per faciles transformationes ex iis fit

$$t + u(\alpha + \alpha^4) = (\alpha + \alpha^4)^n, \quad \varphi(\alpha) = \pm\alpha^k(\alpha + \alpha^4)^n,$$

itaque pro $\lambda = 5$ unitates complexae omnes unius unitatis fundamentalis potestates existunt, quae praeterea unitatibus simplicibus formae $\pm\alpha^k$ multiplicatae esse possunt, praeter has autem aliae non dantur. Pro majoribus numeris λ unitatum omnium indagatio multo difficilior est, et principia peculiaria poscit, quae nos hactenus nondum satis perscrutati sumus. Eo magis hac quaestione nobis supersedendum videtur, quum compertum habeamus Cl. Lejeune-Dirichlet recentissimo tempore in Italia, ubi etiam nunc versatur, de iis unitatibus complexis theoremata fundamentalia elaborasse, quae ut propediem in publicum edat cum desiderio exspectamus. Hic etiam adnotabo geometram juvenilem Leopoldum Kronecker, qui nunc Vratislaviae litteris mathematicis studet, pro absolvendis iis unitatibus quae ad numerum $\lambda = 7$ pertinent methodum subtilem invenisse, quae ni fallor felici successu ad altiorum ordinum unitates pertractandas applicari poterit.

§ 5.

Progredimur ad perscrutandos eos numeros complexos, quorum norma sit numerus primus p, ita ut habeatur

$$p = f(\alpha) f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1}).$$

Numerus primus, qui tali modo in $\lambda - 1$ factores dissolvi potest, secundum theorema paragrapho tertia propositum, formam linearem $m\lambda + 1$ habere debet, nisi est ipse numerus $\lambda = p$, qui talimodo in $\lambda - 1$ factores dissolvitur:

$$\lambda = (1-\alpha)(1-\alpha^2)(1-\alpha^3) \ldots (1-\alpha^{\lambda-1}).$$

Factores $f(\alpha)$, $f(\alpha^2)$ etc., sunt numeri complexi primi qui, si unitates complexae excluduntur, ulterius in factores dissolvi non possunt. Nam si ponimus $f(\alpha)$ e factoribus $\varphi(\alpha) \cdot \psi(\alpha)$ constare, habemus $f(\alpha) = \varphi(\alpha) \cdot \psi(\alpha)$, et $Nf(\alpha) = N\varphi(\alpha) \cdot N\psi(\alpha)$, et quia $Nf(\alpha) = p$ est numerus primus, alter factorum realium integrorum $N\varphi(\alpha)$ et $N\psi(\alpha)$ unitati aequalis esse debet, itaque alter factorum $\varphi(\alpha)$ et $\psi(\alpha)$ erit unitas complexa, et $f(\alpha)$ numerus primus complexus. Porro demonstramus *hos factores $f(\alpha)$, $f(\alpha^2)$ etc., omnes inter se diversos esse.* Ex aequalitate duorum factorum $f(\alpha^\mu) = f(\alpha^\nu)$, alia radice idonea loco α substituta, sequeretur $f(\alpha) = f(\alpha^n)$, et repetita substitutione α^n loco α, esset $f(\alpha) = f(\alpha^n) = f(\alpha^{n^2}) = f(\alpha^{n^3}) =$ etc. Jam si infima potestas numeri n, quae unitati congrua sit modulo λ, est n^h in producto $\lambda - 1$ factorum numeri p erunt h factores aequales, alia deinde radice substituta, quae inter radices α, α^n, α^{n^2} etc. non invenitur, statim alios h factores aequales obtinemus et ita porro, usque dum omnes factores exhausti sunt. Igitur ex aequalitate duorum factorum primum sequeretur ut p sit potestas h^{te} producti eorum factorum complexorum, qui inter se diversi sint. Radices α, α^n, α^{n^2} etc. periodum h terminorum efficiunt, atque si functio rationalis integra $f(\alpha)$, loco α omnibus periodi radicibus substitutis, immutata manet, hanc ipsam omnium similium periodorum, itaque etiam unius earum, functionem rationalem integram esse constat. Ceteri factores diversi ab hoc non differre possunt, nisi quod ceterarum periodorum functiones sunt, et omnium factorum diversorum productum, tanquam functio invariabilis omnium periodorum similium, esse debet numerus integer realis. Hinc tandem sequeretur ut p esset potestas numeri realis et exponentis h, quod quum absurdum sit concludimus omnes illos factores primos complexos numeri p inter se diversos esse.

Si tali factore primo complexo numeri p tanquam modulo sive divisore utimur, simul productum ceterorum factorum:

$$F(\alpha)=f(\alpha^2).f(\alpha^3)\ldots.f(\alpha^{\lambda-1})$$

cujus auxilio divisio per numerum complexum $f(\alpha)$ ad divisionem per numerum realem $Nf(\alpha)$ reducitur, magni momenti est, quam ob rem hujus producti proprietates principales praeterire non possumus. Sit $p=f(\alpha)F(\alpha)$ et producto $F(\alpha)$ per multiplicationem evoluto habeatur

$$F(\alpha)=A+A_1\alpha+A_2\alpha^2+\ldots.+A_{\lambda-1}\alpha^{\lambda-1}$$

unde etiam

$$F(\alpha^2)=A+A_1\alpha^2+A_2\alpha^4+\ldots.+A_{\lambda-1}\alpha^{2\lambda-2}$$
$$F(\alpha^3)=A+A_2\alpha^3+A_2\alpha^6+\ldots.+A_{\lambda-1}\alpha^{3\lambda-3}$$
$$\vdots$$
$$F(\alpha^{\lambda-1})=A+A_1\alpha^{\lambda-1}+A_2\alpha^{2\lambda-2}+\ldots.+A_{\lambda-1}\alpha^{(\lambda-1)(\lambda-1)}$$

iis aequationibus secundum ordinem per α^{-n}, α^{-2n}, $\alpha^{-3n}\ldots.\alpha^{-(\lambda-1)n}$ multiplicatis et additione conjunctis, habemus

$$\alpha^{-n}F(\alpha)+\alpha^{-2n}F(\alpha^2)+\ldots+\alpha^{-(\lambda-1)n}F(\alpha^{\lambda-1})=\lambda A_n-(A+A_1+A_2+\ldots+A_{\lambda-1})$$

inde mutando n in $n-1$ et subtrahendo

$$\alpha^{-n}(1-\alpha)F(\alpha)+\alpha^{-2n}(1-\alpha^2)F(\alpha^2)+\ldots.+\alpha^{-(\lambda-1)n}F(\alpha^{\lambda-1})=\lambda(A_n-A_{n-1})$$

ex hac forma, denuo mutato n in $n+1$ et $n+2$, prodeunt similes formae pro $\lambda(A_{n+1}-A_n)$ et $\lambda(A_{n+2}-A_{n+1})$, quibus inter se multiplicatis formetur evolutio formae

$$\lambda^2(A_{n+1}-A_n)^2-\lambda^2(A_{n+2}-A_{n+1})(A_n-A_{n-1}).$$

Facile perspicitur in hac evolutione quadrata numerorum complexorum $F(\alpha)$, $F(\alpha^2)$ etc. non reperiri, sed sola producta binorum diversorum, quae factores $f(\alpha)f(\alpha^2)f(\alpha^3)\ldots.f(\alpha^{\lambda-1})$ omnes simul, ideoque factorem realem p continent. Quum igitur p sit factor communis omnium terminorum hujus formulae evolutae, factore λ^2 omisso, habemus congruentiam

$$(A_{n+1}-A_n)^2\equiv(A_{n+2}-A_{n+1})(A_n-A_{n-1}) \text{ mod. } p$$

quae etiam hoc modo repraesentari potest:

$$\frac{A_{n+1}-A_n}{A_{n+2}-A_{n+1}}\equiv\frac{A_n-A_{n-1}}{A_{n+1}-A_n} \text{ mod. } p$$

posito igitur

$$\frac{A_{n+1}-A_n}{A_{n+2}-A_{n+1}} \equiv \xi \mod p$$

videmus numerum ξ pro omnibus diversis numeris n eundem manere. Hanc congruentiam si hoc modo scribimus

$$A_{n+1}\xi - A_n \equiv A_{n+2}\xi - A_{n+1} \mod p$$

videmus etiam $A_{n+1}\xi - A_n \equiv \eta \mod p$ pro omnibus diversis numeris n non variari, itaque habemus congruentias

$$(A)\qquad \begin{array}{llll} A\xi & -A_{\lambda-1} & \equiv\eta & \\ A_1\xi & -A & \equiv\eta & \\ A_2\xi & -A_1 & \equiv\eta & \ldots \mod p \\ \vdots & & \vdots & \\ A_{\lambda-1}\xi & -A_{\lambda-2} & \equiv\eta & \end{array}$$

Aliud etiam systema congruentiarum, quibus coëfficientes producti $F(\alpha)$ satisfacere debent, facile e congruentia

$$A_{n+1}\xi - A_n \equiv A_{n+2}\xi - A_{n+1} \mod p \text{ deducitur:}$$

$$(B)\qquad \begin{array}{ll} A_{\lambda-1} - A & \equiv (A-A_1)\xi \\ A_{\lambda-2} - A_{\lambda-1} & \equiv (A-A_1)\xi^2 \\ A_{\lambda-3} - A_{\lambda-2} & \equiv (A-A_1)\xi^3 \\ \vdots & \vdots \\ A_1 - A_2 & \equiv (A-A_1)\xi^{\lambda-1} \end{array}$$

quibus additis, omisso factore $A - A_1$, qui nihilo congruus esse non potest, sequitur ut ξ sit una $\lambda - 1$ radicum realium congruentiae

$$1 + \xi + \xi^2 + \xi^3 + \ldots + \xi^{\lambda-1} \equiv 0 \mod p.$$

§ 6.

Singulis congruentiis (A) paragraphi antecedentis secundum ordinem quo scriptae sunt factoribus $1, \alpha, \alpha^2, \ldots \alpha^{\lambda-1}$ multiplicatis, earum summa facile in hanc formam redigitur:

$$(\xi - \alpha)(A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1}) \equiv 0 \mod p$$

sive

$$(\xi - \alpha) F(\alpha) \equiv 0 \mod p.$$

et factore communi $F(\alpha)$ e modulo $p = f(\alpha) \cdot F(\alpha)$ et ex ipsa congruentia sublato habemus

$$\xi - \alpha \equiv 0 \mod. f(\alpha)$$

unde elucet etiam pro quolibet numero complexo $\varphi(\alpha)$ semper esse

$$\varphi(\alpha) \equiv \varphi(\xi) \mod. f(\alpha)$$

itaque nacti sumus theorema insigne: *Pro modulo complexo $f(\alpha)$, cujus norma est numerus primus, omnes numeri complexi realibus numeris congrui sunt.* Hoc theorema omnibus congruentiis numerorum complexorum, quarum modulus normam habet numerum primum, viam patefacit, quam vero patefactam hic statim relinquimus.

E congruentia $\alpha \equiv \xi \mod. f(\alpha)$ sequitur $f(\alpha) \equiv f(\xi) \mod. f(\alpha)$, itaque $f(\xi) \equiv 0 \mod. f(\alpha)$, numerus autem integer realis $f(\xi)$, qui factorem $f(\alpha)$ continet, omnes etiam factores huic conjunctos, ideoque factorem p continere debet, unde concludimus eam esse indolem factorum complexorum numeri p, ut certa radice congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \mod. p$. loco α substituta, horum factorum unus per p divisibilis fiat. Praeterea adnotamus pro quolibet numero ξ unum, non plures, factorum $f(\xi), f(\xi^2), f(\xi^3)$ etc. per p divisibilem esse, si enim simul esset $f(\xi) \equiv 0$ et $f(\xi^r) \equiv 0 \mod. p$, per congruentiam $\xi \equiv \alpha \mod. f(\alpha)$ etiam esse deberet $f(\alpha^r) \equiv 0 \mod. f(\alpha)$, duo igitur factores $f(\alpha)$ et $f(\alpha^r)$ aequales esse deberent, quod fieri non posse supra demonstravimus. Quum radices congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \mod. p$ omnes tanquam potestates unius radicis repraesentari possint, alia quacunque radice loco ξ substituta, alium etiam factorem producti $f(\xi) \cdot f(\xi^2), f(\xi^3) \ldots f(\xi^{\lambda-1})$ per p divisibilem fieri patet, *singuli igitur $\lambda - 1$ factores $f(\alpha) f(\alpha^2) \ldots f(\alpha^{\lambda-1})$ cum singulis $\lambda - 1$ radicibus congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0$ ita conjuncti sunt, ut pro certa radice ξ certus etiam illorum factorum, si ξ loco α substituitur, per p divisibilis fiat, idemque sit divisor numeri $\xi - \alpha$.*

Jam eo pervenimus ut quaestionem gravissimam absolvere possimus: utrum plures numeri complexi eandem normum, quae numerus primus est, habere possint an non, sive an idem numerus primus p, pluribus modis diversis in $\lambda - 1$ factores primos complexos dissolvi possit. Fingamus duos numeros complexos $f(\alpha)$ et $\varphi(\alpha)$ eandem normam p, numerum primum, habere, ita ut sit

$$p = f(\alpha) f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1})$$
$$p = \psi(\alpha) \psi(\alpha^2) \psi(\alpha^3) \ldots \psi(\alpha^{\lambda-1}).$$

Quum singuli factores horum productorum ad singulas radices congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \mod p$ pertineant, alterius producti factores ita dispositos accipiamus, ut $\psi(\alpha)$ et $f(\alpha)$ ad eandem radicem ξ pertineant, quo facto uterque etiam erit divisor numeri $\xi - \alpha$ atque $\psi(\xi) \equiv 0$, $f(\xi) \equiv 0 \mod p$. Inde positis

$$\psi(\alpha) = c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1}$$

$$F(\alpha) = f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1}) = A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1}$$

$$\text{et } \psi(\alpha) \cdot F(\alpha) = C + C_1\alpha + C_2\alpha^2 + \ldots + C_{\lambda-1}\alpha^{\lambda-1}$$

hoc producto per multiplicationem evoluto habemus:

$$\begin{aligned}
C &= Ac + A_{\lambda-1}c_1 + A_{\lambda-2}c_2 + \ldots + A_1c_{\lambda-1} \\
C_1 &= A_1c + Ac_1 + A_{\lambda-1}c_2 + \ldots + A_2c_{\lambda-1} \\
&\vdots \qquad\qquad \vdots \\
C_{\lambda-1} &= A_{\lambda-1}c + A_{\lambda-2}c_1 + A_{\lambda-3}c_2 + \ldots + Ac_{\lambda-1}
\end{aligned}$$

et si harum aequationum binae contiguae subtrahuntur:

$$\begin{aligned}
C - C_1 &= (A - A_1)c + (A_{\lambda-1} - A)c_1 + (A_{\lambda-2} - A_{\lambda-1})c_2 + \ldots + (A_1 - A_2)c_{\lambda-1} \\
C_1 - C_2 &= (A_1 - A_2)c + (A - A_1)c_1 + (A_{\lambda-1} - A)c_2 + \ldots + (A_2 - A_3)c_{\lambda-1} \\
&\vdots \qquad\qquad \vdots \\
C_{\lambda-2} - C_{\lambda-1} &= (A_{\lambda-2} - A_{\lambda-1})c + (A_{\lambda-3} - A_{\lambda-2})c_1 + (A_{\lambda-1} - A_{\lambda-3})c_2 + \ldots + (A_{\lambda-1} - A)c_{\lambda-1}
\end{aligned}$$

quae per congruentias (*B*) § 5 mutantur in

$$\begin{aligned}
C - C_1 &\equiv (A - A_1)(c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1}) \\
C_1 - C_2 &\equiv (A_1 - A_2)(c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1}) \mod p \\
&\vdots \qquad\qquad \vdots \\
C_{\lambda-2} - C_{\lambda-1} &\equiv (A_{\lambda-2} - A_{\lambda-1})(c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1})
\end{aligned}$$

et quum sit $\psi(\xi) = c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1} \equiv 0 \mod p$, habemus

$$C \equiv C_1 \equiv C_2 \equiv \ldots \equiv C_{\lambda-1}, \mod p$$

unde sequitur ut productum $\psi(\alpha) \cdot F(\alpha)$ per p divisibile sit, itaque ponere licet

$$\psi(\alpha) \cdot F(\alpha) = p\ \varphi(\alpha)$$

et quum sit $p = f(\alpha) \cdot F(\alpha)$, factore communi $F(\alpha)$ sublato habemus

$$\varphi(\alpha) = f(\alpha) \cdot \varphi(\alpha)$$

unde etiam

$$N\psi(\alpha) = Nf\alpha)\, N\varphi(\alpha)$$

et quia $Nf(\alpha) = N\psi(\alpha) = p$, hoc factore omisso est

$$N\varphi(\alpha) = 1$$

ergo $\varphi(\alpha)$ est unitas complexa, atque habemus theorema: *Omnes numeri complexi ejusdem normae, quae numerus primus est, non inter se differunt nisi unitatibus complexis, quibus multiplicatae esse possunt.* Ad diverstitatem numerorum conjunctorum, quae obvia est, hic non respicimus. Idem theorema etiam hoc modo enuntiari potest: *Si numerus primus realis aliquo modo in* $\lambda - 1$ *factores complexos dissolvi potest, idem semper infinitis aliis modis tanquam productum* $\lambda - 1$ *factorum complexorum repraesentari potest, qui vero e factoribus unius repraesentationis, unitatum complexarum ope, omnes eruuntur.*

§ 7.

Facile inveniuntur numeri complexi, quorum normae factorem p, numerum primum formae $m\lambda + 1$, implicant. Nam *si* ξ *est radix aliqua congruentiae* $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0$ *mod.* p, *et si coëfficientes numeri complexi* $\psi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$ *congruentiae* $a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1} \equiv 0$ *satisfaciunt, semper est* $N\psi(\alpha) \equiv 0$ mod. p. Etenim si ponimus $a_1(\xi - \alpha) + a_2(\xi^2 - \alpha^2) + a_3(\xi^3 - \alpha^3) + \ldots + a_{\lambda-1}(\xi^{\lambda-1} - \alpha^{\lambda-1}) = pP - \psi(\alpha)$ et si alteri parti hujus aequationis forma datur $(\xi - \alpha)\varphi(\alpha)$ est

$$\psi(\alpha) = pP - (\xi - \alpha)\varphi(\alpha)$$

cujus numeri complexi normam factorem p habere patet siquidem, quod posuimus, norma numeri $\xi - \alpha$, i. e. $1 + \xi + \xi^2 + \ldots \xi^{\lambda-1}$ per p divisibilis est.

Hujus theorematis ope *omnes* numeros complexos inveniri, quorum normae factorem p habeant, inde apparet, quod theorema inversum etiam valet, scilicet: *Si norma numeri complexi* $\psi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$ *factorem* p *implicat, semper datur radix aliqua* ξ *congruentiae* $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0$ *mod.* p, *quae numerum* $\psi(\xi) = a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1}$ *per* p *divisibilem reddat.* Consideremus hanc functionem rationalem integram variabilis x:

$$\psi(x)\psi(x^2)\psi(x^3)\ldots\psi(x^{\lambda-1}) - N\psi(\alpha)$$

quae quum manifesto evanescat pro $x = \alpha, \alpha^2, \alpha^3, \ldots \alpha^{\lambda-1}$, factorem $1 + x + x^3 + \ldots + x^{\lambda-1}$ habere debet, eamque ob causam, si x radici alicui congruentiae $1 + x + x^2 + \ldots + x^{\lambda-1} \equiv 0$ mod. p aequalis ponitur per p divisibisis est; inde si hujus congruentiae radicem aliquam, uti supra fecimus, littera ξ denotamus, semper unus factorum producti $\psi(\xi)\psi(\xi^2)\psi(\xi^3)\ldots\psi(\xi^{\lambda-1})$ per p divisibilis esse

debet. Praeterea quia omnes radices illius congruentiae unius radicis ξ potestates sunt, sponte apparet pro alia radice ξ alium etiam factorem hujus producti per p divisibilem fieri, itaque pro quolibet factore certa quaedam radix ξ exstare debet, qua substituta nihilo congruus reddatur.

§ 8.

Postquam demonstravimus quo modo infinitus numerus complexorum numerorum omnium inveniatur, quorum normae factorem p habeant, quaerendum nobis videtur an semper inter hos numeros complexos exstent quarum norma sit ipse numerus p, sive quod idem est, an quilibet numerus primus p formae $m\lambda + 1$ in $\lambda - 1$ factores primos conjunctos diffindi possit. Ad hunc finem ponamus esse $p = f(\alpha) f(\alpha^2) f(\alpha^3) \ldots . f(\alpha^{\lambda-1})$, et videamus quae inde pro numero p sequantur. Hujus producti factores secundum radices unitatis $\alpha, \alpha^2, \alpha^3, \ldots . \alpha^{\lambda-1}$, quas continent in periodos dividamus. Productum factorum eorum qui ad eandem periodum pertinent, ex notis Cl. Gaussii theorematis, erit functio rationalis integra linearis omnium periodorum similium. Jam si $\lambda - 1$ factoribus e et f constat, et e periodi f terminorum accipiuntur, quas Gaussii signis designamus $(f,1)$, (f,g), $(f,g^2) \ldots . (f,g^{e-1})$, productum eorum factorum, qui eandem periodum constituunt hanc formam habet:

$$b + b_1 (f,1) + b_2 (f,g) + \ldots . + b_e (f,g^{e-1})$$

et simili modo producta factorum qui ceteras periodos conficiunt

$$b + b_1 (f,g) + b_2 (f,g^2) + \ldots . + b_e (f,1)$$
$$b + b_1 (f,g^2) + b_2 (f,g^3) + \ldots . + b_e (f,g)$$
$$\text{etc.} \qquad \text{etc.}$$

quarum omnium productum quum sit functio invariabilis (symmetrica) omnium periodorum, ab iis periodis liberum est, et formam certam gradus e et $e+1$ indeterminatorum $b, b_1, b_2, \ldots . b_e$ efficit, qui facile ad e indeterminatos numeros reducuntur. Igitur si $e, e', e'' \ldots .$ sunt divisores numeri $\lambda - 1$, numerus p repraesentari debet per formam certam gradus e et e indeterminatorum, idemque per formam gradus e' et e' indeterminatorum etc. Hoc autem pro certis numeris p et λ fieri non posse facillime intelligitur ex forma secundi gradus et duorum indeterminatorum, quam p habere debet, si in $\lambda - 1$ factores

primos complexos diffindi potest; duae enim periodi, quarum altera ad residua quadratica, altera ad nonresidua pertinet, valores habent $\frac{-1+\sqrt{\pm\lambda}}{2}$ et $\frac{-1-\sqrt{\pm\lambda}}{2}$, inde productum ex altera semissi factorum complexorum numeri p compositum hanc formam habebit $\frac{a\pm b\sqrt{\pm\lambda}}{2}$ et ipse numerus p habebit formam $p = \frac{a^2 \mp \lambda b^2}{4}$ seu $4p = a^2 \mp \lambda b^2$, quam numeri formae $m\lambda + 1$ non semper patiuntur, siquidem praeter formam principalem aliae quoque formae non aequivalentes secundi gradus, determinantis $\mp\lambda$, locum habent. Simili modo etiam altiorum graduum formae impedimento esse possunt, quominus numerus p in $\lambda - 1$ factores primos complexos dissolvi queat.

Quia numeri primi reales formae $m\lambda + 1$ non semper tanquam producta $\lambda - 1$ factorum complexorum repraesentari possunt, multis etiam numerorum integrorum realium proprietatibus simplicibus numeri complexi carent. Pro iis generaliter non valet propositio fundamentalis ut quilibet numerus sit productum factorum complexorum simplicium, qui neglectis unitatibus complexis semper iidem sint, re enim vera nonnunquam idem numerus compositus pluribus modis diversis in factores simplices complexos diffindi potest. Eadem res etiam hoc modo enuntiari potest: si numerus complexus per alium numerum complexum ita dividi potest, ut quotiens sit integer complexus, factores simplices divisoris non ubique cum factoribus simplicibus dividendi compensari possunt. Quod ut demonstremus denuo numerum ξ cognitae illius congruentiae radicem in auxilium vocamus, quae hoc modo in factores dissolvitur: $(\xi - \alpha)(\xi - \alpha^2) \ldots (\xi - \alpha^{\lambda-1}) \equiv 0 \mod p$. Jam si factores divisoris p cum factoribus dividendi tollerentur, p cum aliquo factorum $\xi - \alpha$, $\xi - \alpha^2$ etc., factorem communem haberet, ideoque etiam cum singulo quoque. Sit $f(\alpha)$ hic factor communis numerorum p et $\xi - \alpha$, $f\alpha^2$ erit factor communis numerorum p et $\xi - \alpha^2$, et ita porro; omnes igitur numeri complexi conjuncti $f(\alpha), f(\alpha^2) \ldots f(\alpha^{\lambda-1})$ factores essent numeri p, omnesque inter se diversi, quia $\xi - \alpha$, $\xi - \alpha^2$ etc., non possunt factores communes habere nisi eos quorum norma sit 1 vel λ scilicet $\alpha - \alpha^2$, $\alpha - \alpha^3$ etc. Inde sequeretur ut quilibet numerus primus $p = m\lambda + 1$ esset productum $\lambda - 1$ factorum complexorum conjunctorum, quod in universum non pro omnibus valoribus numerorum p et λ valere supra demonstravimus. Maxime dolen-

dum videtur, quod haec numerorum realium virtus, ut in factores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quae si esset tota haec doctrina, quae magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset. Eam ipsam ob causam numeri complexi, quos hic tractamus, imperfecti esse videntur, et dubium inde oriri posset, utrum hi numeri complexi ceteris qui fingi possint praeferendi, an alii quaerendi essent, qui in hac re fundamentali analogiam cum numeris integris realibus servarent. Attamen hi numeri complexi qui unitatis radicibus et numeris integris realibus componuntur, non ex arbitrio facti sunt, sed ex ipsa doctrina numerorum procreati, atque ipsorum ea ratio est, ut in doctrina sectionis circuli et residuorum potestatum altiorum ulterius promovenda iis carere nullo modo possimus.

§ 9.

Quum numerorum primorum formae $m\lambda + 1$ alii in $\lambda - 1$ factores complexos discerpi possint, alii non possint, e re est ut inveniatur qui et quales sint ii numeri λ et p, pro quibus talis repraesentatio locum habet, atque ut pro iis qui minorem tantum numerum factorum primorum habent, horum factorum numerus et forma propria indagetur, quod vero problema ulterioribus virorum doctorum perscrutationibus relinquendum est. Ipse ut hanc rem accuratius cognoscerem, et ut exemplis docerer, omnium numerorum primorum infra mille, qui formas habent

$5m + 1$, $7m + 1$, $11m + 1$, $13m + 1$, $17m + 1$, $19m + 1$ et $23m + 1$

factores primos computavi, et methodos quibus usus sum et ipsos factores primos computatos hoc loco in publicum edam.

Altera methodus factore communi duorum numerorum complexorum inveniendo nititur, quod problema simili modo solvendum est atque pro numeris integris realibus. Si $\varphi(\alpha)$ et $f(\alpha)$ sunt numeri complexi quorum factor communis maximus investigandus est, et $N\varphi(\alpha) > Nf(\alpha)$, a numero fracto $\frac{\varphi(\alpha)}{f(\alpha)}$ numerum certum integrum subtraho $\psi(\alpha)$, quem siquidem fieri potest ita eligo, ut norma residui sit minor unitate, sive

$$N\left(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\right) < 1.$$

Ut hoc efficiatur evolvo productum $F(\alpha) = f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1})$ ejusque auxilio etiam productum

$$\varphi(\alpha) F(\alpha) = C + C_1 \alpha + C_2 \alpha^2 + \ldots + C_{\lambda-1} \alpha^{\lambda-1}$$

porro accipio $\psi(\alpha) = c + c_1 \alpha + c_2 \alpha^2 + \ldots + c_{\lambda-1} \alpha^{\lambda-1}$, et simpliciter scribo n loco $Nf(\alpha)$. Inde erit

$$\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha) = \frac{\varphi(\alpha) F(\alpha)}{n} - \psi(\alpha)$$

et posito

$$\frac{\varphi(\alpha) F(\alpha)}{n} - \psi(\alpha) = k + k_1 \alpha + k_2 \alpha^2 + \ldots + k_{\lambda-1} \alpha^{\lambda-1}$$

erit

$$k = \frac{C}{n} - c, k_1 = \frac{C_1}{n} - c_1, k_2 = \frac{C_2}{n} - c_2 \text{ etc.}$$

Jam numeros c, c_1, c_2 etc. ita eligo ut integri maximi sint, qui singulis fractionibus $\frac{C}{n}, \frac{C_1}{n}, \frac{C_2}{n}$ etc., contineantur, quo facto numeri k, k_1, k_2 etc., omnes erunt positivi et minores unitate. Certo talis numeri complexi $k + k_1 \alpha + k_2 \alpha^2 + \ldots + k_{\lambda-1} \alpha^{\lambda-1}$ norma parva erit, sed semper eam unitate minorem fore nondum liquet, neque etiam semper res ita se habet. Hoc autem loco nobis notandum est numeros k, k_1, k_2 etc., iis conditionibus quas posuimus nondum plane determinatos esse, omnibus enim coëfficientibus C, C_1, C_2 etc., eodem numero auctis, $\varphi(\alpha) \cdot F(\alpha)$ non mutatur, sed numeri integri maximi, qui fractionibus $\frac{C}{n}, \frac{C_1}{n}, \frac{C_2}{n}$ etc., insunt, revera mutari possunt. Nam si numeros C, C_1, C_2 etc. omnes aqualiter crescentes accipimus, numeri k, k_1, k_2 etc., omnes eodem modo crescent, usque dum maximus eorum unitatem superaverit, quo facto unitate minuendus est, et subito omnium minimus fit. Eadem mutatione repetita patet in universum obtineri λ numeros complexos $k + k_1 \alpha + k_2 \alpha^2 + \ldots + k_{\lambda-1} \alpha^{\lambda-1}$, quorum normae diversae sint. Jam si vel omnium harum normarum nulla unitate minor existet, methodus nostra nos deficit, hunc autem defectum non methodo vitio dandum, sed rei ipsius natura necessarium esse, infra demonstrabitur. Si vero, quod fere semper evenire solet, talis norma unitate minor fit, habemus

$$N\left(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\right) < 1 \text{ ideoque } N(\varphi(\alpha) - f(\alpha)\psi(\alpha)) < Nf(\alpha).$$

Posito $\varphi(\alpha) - f(\alpha)\psi(\alpha) = R(\alpha)$ patet factorem maximum communem numerorum $\varphi(\alpha)$ et $f(\alpha)$ eundem esse numerorum $f(\alpha)$ et $R(\alpha)$, unde indagatio factoris communis eo reducta est, ut aliorum duorum numerorum, quorum normae minores sunt, factor communis quaerendus sit. Itaque hac methodo repetita, nisi forte casus ille adversus evenit, quem supra commemoravimus, tandem ad duos numeros pervenimus, quorum alter factor alterius, ideoque hic ipse factor communis est quem quaerimus; cujus norma si unitas est, numeri illi sunt inter se primi.

Facile haec methodus ad factores primos numeri $p = m\lambda + 1$ indagandos applicari potest, siquidem p revera est productum $\lambda - 1$ factorum conjunctorum. Quem ad finem quaeratur radix aliqua ξ congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0$ mod. p, quae si p in $\lambda - 1$ factores conjunctos diffindi potest, semper talis est, ut $\xi - \alpha$ et p factorem complexum communem habeant. Hic igitur, secundum methodum traditam inventus, erit factor simplex complexus numeri p. Supra vidimus pro certis numeris p et λ talem factorem communem numerorum $\xi - \alpha$ et p non adesse, quamvis norma numeri $\xi - \alpha$ per p divisibilis sit, porro si per methodum traditam numeri complexi normarum minorum quaeruntur, patet eorum omnium normas per p divisibiles esse, quam ob rem nullo modo ad normam unitatem pervenire possumus, semper igitur factor communis ab unitate diversus inveniretur, etiam ubi talem factorem non adesse demonstravimus, nisi in omnibus iis calculis eveniret ut norma istius numeri complexi fracti $k + k_1\alpha + k_2\alpha^2 + \ldots + k_{\lambda-1}\alpha^{\lambda-1}$ minor unitate fieri non posset, qua conditione methodus nostra ad finem propositum perducere non potest.

Altera methodus minus quidem directa tamen multo faciliori negotio factores primos complexos numeri $p = m\lambda + 1$ praebet. In hac omnes congruentiae $1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0$ mod. p radices ξ, ξ^2, ξ^3 etc., in usum vocamus, quibus e canone arithmetico a Cl. Jacobi edito depromtis, sive alio modo inventis, solutiones congruentiae $a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1} \equiv 0$ mod. p quaerimus, ex quovis systemate numerorum $a, a_1, a_2, \ldots a_{\lambda-1}$, qui huic congruentiae satisfaciunt numerum complexum $f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$ componimus, et ex omnibus iis numeris, quarum normae per theorema supra demonstratum § 7. factorem p habent, eam eligimus quae simplicissima sit, et normam quam minimam habere videatur, quae jam ipsa computanda est, ut appareat utrum revera

ipsi numero p an multiplo ejus aequalis sit. Si eveniret hanc normam non esse ipsum p, sed ejus multiplum e numeris complexis quarum normae per p divisibiles sunt alius quaerendus et examinandus esset, et ita porro. Si vero horum numerorum complexorum nullus ipsam normam p habet, hic numerus primus p iis adnumerandus est, qui $\lambda - 1$ factoribus complexis conjunctis non sunt compositi.

§ 10.

Antequam ipsos numerorum primorum realium factores primos complexos quos invenimus literis consignamus pauca de iis praemittere convenit. Pro $\lambda = 5$, 7, 11, 13, 17 et 19 omnes numeros primos formae $m\lambda + 1$ in primo mille contentos in $\lambda - 1$ factores dissolvimus, primus numerus λ, pro quo hoc genus factorum primorum non semper datur, est numerus $\lambda = 23$; inter octo enim numeros primos formae $23m + 1$, qui minores sunt quam mille, tres sunt qui viginti duobus factoribus primis constant, reliquos autem quinque, qui quum formam quadraticam $4p = a^2 + 23b^2$ non patiantur, in viginti duo factores conjunctos dissolvi non possunt, in undecim factores primos complexos discerpere nobis contigit. Tales numeri eundem characterem habere videntur ac numeri primi qui non sunt formae $m\lambda + 1$, quos de hac nostra commentatione exclusimus, hi omnes habent minorem numerum factorum complexorum primorum, qui non tam radicum singularum aequationis $\alpha^\lambda = 1$ quam periodorum functiones lineares sunt. Simili enim modo horum quinque numerorum primorum factores primi complexi, quos invenimus, periodos binarum radicum continent. Quibus praemissis ipsos factores inventos tradimus.

1) Si $\lambda = 5$, et α radix aequationis $\alpha^5 = 1$.

$11 = N(2 + \alpha)$
$31 = N(2 - \alpha)$
$41 = N(3 + 2\alpha + \alpha^2)$
$61 = N(3 + \alpha)$
$71 = N(3 - \alpha + \alpha^2)$
$101 = N(3 + \alpha - \alpha^2)$
$131 = N(3 + \alpha - \alpha^4)$
$151 = N(3 + 2\alpha - \alpha^4)$
$181 = N(4 + 3\alpha)$
$191 = N(4 + \alpha + 2\alpha^2)$
$211 = N(3 - 2\alpha)$
$241 = N(4 - \alpha + \alpha^2)$
$251 = N(5 + 2\alpha + \alpha^4)$
$271 = N(3 - 3\alpha + \alpha^2)$
$281 = N(4 + \alpha - \alpha^2)$
$311 = N(5 + 3\alpha + 2\alpha^2 + \alpha^3)$

$331 = N(4 - 2\alpha + \alpha^2)$
$401 = N(4 + 3\alpha - \alpha^4)$
$421 = N(5 + 2\alpha + 2\alpha^2) = N(5+2\alpha)$
$431 = N(4 - 2\alpha - \alpha^4)$
$461 = N(4 - \alpha - \alpha^2) = N(5+4\alpha)$
$491 = N(5 + 3\alpha + \alpha^3)$
$521 = N(5 + \alpha)$
$541 = N(3 - 3\alpha - \alpha^2)$
$571 = N(6 + 5\alpha + 3\alpha^2)$
$601 = N(5 + 2\alpha - \alpha^2)$
$631 = N(4 - 2\alpha - \alpha^3)$
$641 = N(5 + 3\alpha + 4\alpha^2)$
$661 = N(5 + \alpha - \alpha^2 + 3\alpha^3)$
$691 = N(3 - 3\alpha - 2\alpha^2)$
$701 = N(4 - \alpha - 2\alpha^2 + \alpha^3)$
$751 = N(6 + 4\alpha + 3\alpha^2)$
$761 = N(5 - 2\alpha + \alpha^2)$
$811 = N(3 - 3\alpha - 2\alpha^2 + \alpha^3) = N(6-3\alpha-\alpha^2)$
$821 = N(4 - \alpha - 2\alpha^2 + 2\alpha^3)$
$881 = N(6 + 2\alpha + \alpha^2)$
$911 = N(5 + \alpha^2 - 2\alpha^4)$
$941 = N(4 + 3\alpha - 3\alpha^2 - \alpha^3) = N(6+\alpha+2\alpha^2)$
$971 = N(5 - 2\alpha - \alpha^4)$
$991 = N(6 + \alpha + \alpha^3) = N(6+5\alpha)$

2) Si $\lambda = 7$, et α est radix aequationis $\alpha^7 = 1$.

$29 = N(1 + \alpha - \alpha^2)$
$43 = N(2 + \alpha)$
$71 = N(2 + \alpha + \alpha^3)$
$113 = N(2 - \alpha + \alpha^5)$
$127 = N(2 - \alpha)$
$197 = N(3 + \alpha + \alpha^5 + \alpha^6)$
$211 = N(3 + \alpha + 2\alpha^2)$
$239 = N(3 + 2\alpha + 2\alpha^2 + \alpha^3)$
$281 = N(2 - \alpha - 2\alpha^3)$
$337 = N(2 + \alpha - \alpha^2 - \alpha^4)$
$379 = N(3 + 2\alpha + \alpha^2)$
$421 = N(3 + \alpha + \alpha^2)$
$449 = N(2 + \alpha - \alpha^3 - \alpha^6)$
$463 = N(3 + 2\alpha)$
$491 = N(3 + \alpha + \alpha^3 - \alpha^5)$
$547 = N(3 + \alpha)$
$617 = N(2 + \alpha + \alpha^2 - \alpha^5)$
$631 = N(2 + 2\alpha - \alpha^2 + \alpha^3 + \alpha^6)$
$659 = N(2 + 2\alpha - \alpha^2 + \alpha^5)$
$673 = N(4 + 3\alpha + 2\alpha^2 + \alpha^4 + 2\alpha^6)$
$701 = N(3 + \alpha + \alpha^4 - \alpha^5 + \alpha^6)$
$743 = N(3 + 2\alpha - \alpha^3 - \alpha^4)$
$757 = N(3 + 2\alpha + \alpha^3)$
$827 = N(2 + 2\alpha - \alpha^4 - \alpha^6)$
$883 = N(2 - \alpha^2 - 2\alpha^3 - \alpha^5)$
$911 = N(3 + 2\alpha - \alpha^3 + \alpha^4)$
$953 = N(3 + \alpha - \alpha^2 - \alpha^3)$
$967 = N(2 + 2\alpha - \alpha^3 + 2\alpha^5)$

3) Si $\lambda = 11$, et α est radix aequationis $\alpha^{11} = 1$.

$23 = N(1 + \alpha + \alpha^5)$
$89 = N(1 + \alpha + \alpha^4 + \alpha^6)$
$97 = N(1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5)$
$199 = N1 + \alpha - \alpha^2)$

$331 = N(1-\alpha+\alpha^3+\alpha^5)$ $\quad$ $661 = N(1+\alpha-\alpha^2+\alpha^4-\alpha^8)$

$353 = N(1+\alpha+\alpha^3+\alpha^4-\alpha^7)$ $\quad$ $683 = N(2+\alpha)$

$397 = N(1+\alpha+\alpha^6-\alpha^7)$ $\quad$ $727 = N(1+\alpha+\alpha^3-\alpha^8-\alpha^9)$

$419 = N(1+\alpha-\alpha^2+\alpha^3)$ $\quad$ $859 = N(1+\alpha+\alpha^2+\alpha^3+\alpha^7-\alpha^8)$

$463 = N(1-\alpha-\alpha^2+\alpha^5+\alpha^6)$ $\quad$ $881 = N(1+\alpha+\alpha^2+\alpha^3-\alpha^4-\alpha^7-\alpha^8)$

$617 = N(2+\alpha+\alpha^3+\alpha^{10})$ $\quad$ $947 = N(2+\alpha^3-\alpha^4-\alpha^6)$

$991 = N(2+\alpha+\alpha^3)$

4) Si $\lambda = 13$, et α radix aequationis $\alpha^{14} = 1$.

$53 = N(1+\alpha+\alpha^3)$ $\quad$ $521 = N(1+\alpha-\alpha^{12})$

$79 = N(1-\alpha+\alpha^{10})$ $\quad$ $547 = N(1-\alpha-\alpha^2+\alpha^3+\alpha^6)$

$131 = N(1-\alpha+\alpha^{11})$ $\quad$ $599 = N(1+\alpha-\alpha^7+\alpha^8+\alpha^{11})$

$157 = N(1+\alpha+\alpha^2+\alpha^5)$ $\quad$ $677 = N(1-\alpha-\alpha^4+\alpha^6+\alpha^9)$

$313 = N(1-\alpha+\alpha^3+\alpha^6)$ $\quad$ $959 = N(1+\alpha-\alpha^2-\alpha^5+\alpha^7)$

$443 = N(1+\alpha-\alpha^3+\alpha^8)$ $\quad$ $911 = N(1+\alpha^3+\alpha^5-\alpha^7-\alpha^{11})$

$937 = N(1+\alpha^3-\alpha^7+\alpha^8-\alpha^{10})$

5) Si $\lambda = 17$, et α radix aequationis $\alpha^{17} = 1$.

$103 = N(1+\alpha^2+\alpha^9)$ $\quad$ $443 = N(1+\alpha+\alpha^2+\alpha^3-\alpha^{15})$

$137 = N(1+\alpha-\alpha^3)$ $\quad$ $613 = N(1+\alpha^2-\alpha^3)$

$239 = N(1+\alpha+\alpha^3)$ $\quad$ $647 = N(1+\alpha+\alpha^{13}+\alpha^{15})$

$307 = N(1-\alpha+\alpha^7)$ $\quad$ $919 = N(1+\alpha+\alpha^4+\alpha^5+\alpha^9)$

$409 = N(1-\alpha^3+\alpha^8)$ $\quad$ $953 = N(1+\alpha+\alpha^9-\alpha^{13})$

6) Si $\lambda = 19$, et α radix aequationis $\alpha^{19} = 1$.

$191 = N(1+\alpha+\alpha^{10})$ $\quad$ $457 = N(1+\alpha+\alpha^3)$

$229 = N(1-\alpha-\alpha^5)$ $\quad$ $571 = N(1+\alpha+\alpha^2+\alpha^3-\alpha^5)$

$419 = N(1+\alpha-\alpha^8)$ $\quad$ $647 = N(1-\alpha^2+\alpha^9)$

$761 = N(1-\alpha^2+\alpha^{12})$

7) Si $\lambda = 23$, et α radix aequationis $\alpha^{23} = 1$.

$$599 = N(1 + \alpha^{15} - \alpha^{16}) \qquad 691 = N(1 + \alpha + \alpha^5)$$
$$829 = N(1 + \alpha^{11} + \alpha^{20})$$

reliqui numeri primi formae $23m + 1$ infra mille undecim factoribus primis constant; habet

47	factorem	$\alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^7 + \alpha^{16}$
139	„	$\alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^4 + \alpha^{19}$
277	„	$2 + \alpha + \alpha^{22} + \alpha^7 + \alpha^{16}$
461	„	$\alpha + \alpha^{22} + \alpha^{10} + \alpha^{13} + \alpha^8 + \alpha^{15} + \alpha^9 + \alpha^{14}$
967	„	$2 + \alpha^{11} + \alpha^{12} + \alpha^4 + \alpha^{19}$

§ 11.

Quae de numeris complexis et de eorum factoribus primis commentati sumus ad doctrinam de sectione circuli felicissimo successu applicari possunt. In hac enim doctrina tales numeri complexi eorumque producta maximi momenti sunt, quorum vera indoles in luce clarissima ponitur si in factores primos diffinduntur.

Sit p numerus primus realis formae $m\lambda + 1$, α radix imaginaria aequationis $\alpha^\lambda = 1$, g radix primitiva numeri primi p, et

$$(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \ldots + \alpha^{p-2} x^{g^{p-2}}.$$

Totius fere doctrinae de circuli sectione caput est formae hujus (α, x) potestas exponentis λ, quae a radice x non pendet, sed radicis α functio rationalis integra est, ideoque numerus complexus ejus generis quod supra tractavimus. Ipsa haec formula (α, x), quam Cl. Lagrange primus adhibuit, proprietatibus insignibus gaudet, quarum maximas Cl. Jacobi primus invenit:

$$(\alpha, x)(\alpha^{-1}, x) = p$$

$$\frac{(\alpha^m, x)(\alpha^n, x)}{(\alpha^{m+n}, x)} = \psi(\alpha) = A + A_1 \alpha + A_2 \alpha^2 + \ldots + A_{\lambda-1} \alpha^{\lambda-1}$$

numerus complexus $\psi(\alpha)$ ita semper comparatus est, ut sit

$$\psi(\alpha)\psi(\alpha^{-1}) = p.$$

Inde positis

$$\begin{aligned}
(\alpha,x)\,(\alpha,\ x) &= \psi_1(\alpha)\,(\alpha^2,x)\\
(\alpha,x)\,(\alpha^2,x) &= \psi_2(\alpha)\,(\alpha^3,x)\\
(\alpha,x)\,(\alpha^3,x) &= \psi_3(\alpha)\,(\alpha^4,x)\\
&\vdots \qquad\qquad \vdots\\
(\alpha,x)\,(\alpha^{\lambda-2},x) &= \psi_{\lambda-2}(\alpha)\,(\alpha^{\lambda-1},x)
\end{aligned}$$

iisque aequationibus inter se multiplicatis, adhibita formula $(\alpha,x)(\alpha^{-1},x)=p$, fit

$$(\alpha,x)^\lambda = p\cdot\psi_1(\alpha)\,\psi_2(\alpha)\,\ldots\,\psi_{\lambda-1}(\alpha).$$

Numeri integri complexi, quibus hoc productum constat, $\psi_1(\alpha)$, $\psi_2(\alpha)$ etc., a se invicem ita pendent, ut quamvis non singuli, tamen productum omnium per unum eorum exprimi possit. Tali autem reductione non indigemus, si pro numeris complexis p, $\psi_1(\alpha)$, $\psi_2(\alpha)$ etc., qui compositi sunt, eorum factores primos adhibemus, quo facto repraesentatio formae $(\alpha,x)^\lambda$ solos factores primos conjunctos numeri p continebit. Disquisitionem nostram ad tales numeros primos p restringentes, qui in $\lambda-1$ factores complexos conjunctos diffindi possunt, habemus

$$p = f(\alpha)\,f(\alpha^2)\,f\alpha^3)\,\ldots\,f(\alpha^{\lambda-1})$$

etiam numeri complexi $\psi_1(\alpha)$, $\psi_2(\alpha)$ etc. alios factores primos habere non possunt nisi eos qui in p reperiuntur, est enim pro quolibet numero r: $\psi_r(\alpha)\,\psi_r(\alpha^{-1})=p$ et supra § 6 demonstravimus numerum p, neglectis unitatibus complexis, quibus factores affecti esse possunt, pluribus modis diversis in $\lambda-1$ factores primos dissolvi non posse. Quilibet igitur numerorum $\psi_r(\alpha)$ est productum alterius semissis factorum $f(\alpha)$, $f(\alpha^2)$ etc. et unitas complexa, quae factor accedere potest, si per $\varphi(\alpha)$ designatur, conditioni $\varphi(\alpha)\,\varphi(\alpha^{-1})=1$ satisfacere, ideoque secundum ea quae § 4 invenimus, simplex unitas $\pm\alpha^k$ esse debet. Inde loco factorum compositorum factoribus simplicibus substitutis, hanc formam habemus:

$$(\alpha,x)^\lambda = \pm\alpha^k f(\alpha)^{m_1} f(\alpha^2)^{m_2} f(\alpha^3)^{m_3}\,\ldots\,f\alpha^{\lambda-1)^{m_{\lambda-1}}}$$

in qua m_1, m_2, m_3 etc., sunt exponentes integri positivi, quos jam determinaturi sumus. Primum adhibita formula simplici

$$(\alpha,x)\,(\alpha^{-1},x)=p=f(\alpha)\,f(\alpha^2)\,f(\alpha^3)\,\ldots\,f(\alpha^{\lambda-1})$$

sponte elucet esse $m_1+m_{\lambda-1}=\lambda$, $m_2+m_{\lambda-2}=\lambda$ etc., i. e. summam binorum exponentium, ab initio et a fine aeque distantium, constantem esse et numero λ

aequalem; unde sequitur ut omnes hi exponentes numero λ minores sint. Deinde per formulam generaliorem

$$\frac{(\alpha,x)\,(\alpha^r,x)}{(\alpha^{r+1},x)} = \psi_r(\alpha)$$

fit

$$\frac{f(\alpha)^{m_1} f(\alpha^2)^{m_2} \ldots f(\alpha^{\lambda-1})^{m_{\lambda-1}} \cdot f(\alpha^r)^{m_1} f(\alpha^{2r})^{m_2} \ldots f(\alpha^{r\lambda-r})^{m_{\lambda-1}}}{f(\alpha^r+1)^{m_1} f(\alpha^{2r}+2)^{m_2} \ldots f(\alpha^{(\lambda-1)(r+1)})^{m_{\lambda-1}}} = (\psi_r(\alpha))^\lambda$$

et quia quotiens talium numerorum complexorum, quorum norma est numerus primus, non potest integer esse, nisi singuli factores denominatoris cum factoribus numeratoris compensantur, et quia hic quotiens potestati λ *tae* numeri complexi aequalis est, singulis tribus potestatibus numeri primi $f(\alpha^k)$ in unam conjunctis, facile colligitur pro quolibet numero k esse debere:

$$m_k + m_\mu - m_\nu \equiv 0, \text{ si } \mu \equiv \frac{k}{r}, \quad \nu \equiv \frac{k}{r+1} \text{ mod. } \lambda$$

inde posito $k m_k \equiv n_k$ sive $m_k \equiv \frac{n_k}{k}$ mod. λ fit:

$$m_\mu \equiv \frac{n_\mu}{\mu} \equiv \frac{r\,n_\mu}{k} \text{ et } m_\nu \equiv \frac{n_\nu}{\nu} \equiv \frac{(r+1)n_\nu}{k} \text{ mod. } \lambda$$

iisque substitutis congruentia $m_k + m_\mu - m_\nu \equiv 0$ mutatur in

$$\frac{n_k}{k} + \frac{r \cdot n_k}{k} - \frac{(r+1)n_\nu}{k} \equiv 0 \text{ mod. } \lambda,$$

unde posito $k = 1$ habemus:

$$n_1 + r\,n_\mu - (r+1)n_\nu \equiv 0, \text{ si } \mu \equiv \frac{1}{r} \text{ et } \nu \equiv \frac{1}{r+1} \text{ mod. } \lambda.$$

Jam si primum facimus $r = 1$, fit n_1 aequale numero n cujus index congruus est $\frac{1}{2}$, deinde posito $r = 2$ idem aequalis invenitur numero n cujus index congruus est $\frac{1}{3}$, tum posito $r = 3$ etiam n cujus index $\frac{1}{4}$ illis aequalis invenitur, et ita porro; numeri autem fracti $\frac{1}{1}$, $\frac{1}{2}$, $\frac{1}{3}$ etc., omnibus numeris integris 1, 2, 3 etc., etsi alio ordine, congrui sunt, modulo λ; itaque numeri n pro omnibus indicibus diversis iidem sunt et omitti possunt, quo facto habemus

$$m_k \equiv \frac{n}{k} \text{ mod. } \lambda$$

quae determinatio revera congruentiae $m_k + m_\mu - m_\nu \equiv 0$ pro quolibet valore numerorum k et r satisfacit. Inde habemus theorema insigne: *Si $f(\alpha)$ est factor primus complexus numeri p, cujus norma est ipse numerus p, est*:

$$(C) \ldots . (\alpha,x)^\lambda = \pm\alpha^k f(\alpha)^{m_1} f(\alpha^2)^{m_2} f(\alpha^3)^{m_3} \ldots . f(\alpha^{\lambda-1})^{m_{\lambda-1}}$$

et exponentes m_1, m_2, m_3 etc., ita determinantur ut sint numeri minimi positivi, qui per exponentes potestatum radicis α, ad quos pertinent, multiplicati omnes eidem numero congrui fiant pro modulo λ. Numerus primus complexus $f(\alpha)$, alia radice imaginaria aequationis $\alpha^\lambda = 1$ accepta, etiam signo $f(\alpha^r)$ designari potest, in quo r est numerus integer arbitrarius, quem si ita eligimus ut sit $nr \equiv 1 \bmod \lambda$ exponentes m_1, m_2, m_3 etc. non jam per congruentiam $m_k \equiv \frac{n}{k}$ sed per hanc simpliciorem $m_k \equiv \frac{1}{k} \bmod \lambda$ determinatur; praeterea quum omnes debeant esse minores quam λ, nihil amplius indeterminati relictum est nisi radix α, quae ex omnibus aequationis $\alpha^\lambda = 1$ radicibus imaginariis eligenda sit, et unitas simplex $\pm\alpha^k$ qua hoc productum multiplicatum sit. Inde formae $(\alpha,x)^\lambda$ repraesentatio, quae sectionis circuli caput est, pro omnibus iis numeris p, qui in $\lambda - 1$ factores complexos conjunctos diffindi possunt, ad simplicitatem maximam perducta est. Omnes enim difficultates et calculi longiores eo revocati sunt, ut numeri $p = m\lambda + 1$ factores primi complexi inveniantur, quod methodorum supra traditarum ope facile perficitur. Quum numerus $f(\alpha)$ cujus norma est p, siquidem revera talis numerus datur, non plane determinatus sit, sed semper infinite multis modis diversis exhiberi possit, dubium inde oriri posset, quisnam omnium horum numerorum accipiendus sit, nisi productum illud hac virtute gauderet, ut pro omnibus iis diversis numeris semper idem sit. Facile hoc theorematum paragraphi quartae auxilio demonstratur; nam si $f(\alpha)$ est aliquis numerorum quorum norma est p, ceteros omnes demonstravimus hac forma contineri $f(\alpha)\,\varphi(\alpha)$, in qua $\varphi(\alpha)$ est unitas complexa, inde si $f(\alpha)\,\varphi(\alpha)$ loco $f(\alpha)$ in formula (C) substituitur, accedit factor

$$\varphi(\alpha)^{m_1}\,\varphi(\alpha^2)^{m_2}\,\varphi(\alpha^3)^{m_3} \ldots . \varphi(\alpha^{\lambda-1})^{m_{\lambda-1}} = \Phi(\alpha)$$

Hac unitate $\Phi(\alpha)$ cum reciproca $\Phi(\alpha^{-1})$ multiplicata, quia $m_1 + m_{\lambda-1} = \lambda$, $m_2 + m_{\lambda-1} = \lambda$ etc. fit

$$\Phi(\alpha)\,\Phi(\alpha^{-1}) = (\varphi(\alpha)\varphi(\alpha^2)\varphi(\alpha^3) \ldots . \varphi(\alpha^{\lambda-1}))^\lambda = 1,$$

unitas autem complexa, quae per reciprocam suam multiplicata unitatem realem efficit, simplici unitati $\pm\alpha^n$ aequalis est, itaque quum sit $\Phi(\alpha)=\pm\alpha^n$ videmus solam mutationem levem, quam substitutis aliis numeris complexis $f(\alpha)$ aequationi $Nf(\alpha)=p$ satisfacientibus, formula (C) pati possit, eam esse, ut loco factoris α^k alia quaecunque radix aequationis $\alpha^\lambda=1$ substituenda sit.

Ut methodi in hac paragrapho explicatae indolem veram melius cognoscamus, ad eam respiciamus qua Cl. Gauss usus est in sectione septima disquisitionum arithmeticarum, § 358, ubi casum $\lambda=3$ ingeniosissime pertractavit. Hic totam rem eo reduxit ut numerus $4p$ in formam t^2+27u^2 redigatur, et quum eo pervenisset; problema ab omni parte absolutum esse censuit. Simili modo secundum methodum nostram numerus p in formam certam gradus $\lambda-1$ totidemque indeterminatorum redigi debet, quo facto difficultates omnes sublatae sunt. Quum enim norma sit forma certa gradus $\lambda-1$ et $\lambda-1$ indeterminatorum, talem factorem primum complexum numeri p invenire idem est atque hunc numerum in formam dictam redigere. Si omnes numeri primi p, formae $m\lambda+1$, in hanc formam redigi possent, sive quod idem est, si in $\lambda-1$ factores complexos conjunctos discerpi possent, totius doctrinae de circuli sectione pars major confecta esset, quum vero non omnes numeri p repraesentationem per formam illam patiantur, restat ut etiam pro iis forma propria expressionis $(\alpha,x)^\lambda$ inveniatur. Haec autem res maximis difficultatibus obnoxia est, quae ut superentur magno etiam virorum doctorum labore opus erit.

14

3795
19

This book should be returned to the Library on or before the last date stamped below.

A fine of five cents a day is incurred by retaining it beyond the specified time.

Please return promptly.